

**AFFIDAVIT**

I, Adria Johnson, duly sworn, hereby state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation and have been so employed since April 2011. I am assigned to the Merrillville Resident Agency at the FBI. I am a law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered to investigate and make arrests for violations of U.S. criminal laws. I am assigned to investigate white collar crime and I have been involved in several financial fraud and public corruption investigations, participating in the use of various investigative techniques. As such, I have gained experience in conducting investigations involving violations of Title 18, United States Code, Section 1344 (bank fraud), as well as other fraud. Previous to my service with the FBI, I worked as a supervisor for Casino Surveillance for an Indian Gaming facility. As a Special Agent my responsibilities include investigating possible criminal violations of federal laws.

2. Your affiant states that the facts which establish the probable cause necessary for issuance of the criminal complaint are either personally known to me or have been told to me directly by other law enforcement officers with whom I have worked on this case. This affidavit is being submitted for the limited purpose of establishing probable cause necessary for the issuance of the criminal complaint, and I have not included each and every fact known to me concerning the investigation.

**Overview of the Cracking Cards Bank Fraud Schemes**

3. The Federal Bureau of Investigation, the Internal Revenue Service, and the Federal Deposit Insurance Corporation, in conjunction with other local and federal law enforcement agencies and fraud investigators at several banks, have been investigating bank fraud schemes dubbed "Cracking Cards" by the participants. As detailed below, the investigation

has determined that from August 2011 through September 2013, Cracking Cards schemers deposit counterfeit checks into bank accounts belonging to third parties who willingly or unwillingly surrender their debit cards and PINs for use in the schemes. The schemers then use Automated Teller Machines or point of sale terminals at currency exchanges and retail stores to withdraw or spend funds that the banks advance to the third-party accounts before learning the counterfeit nature of the deposited checks. The banks suffer losses when the checks are found to be counterfeit, and the third-party account holders deny responsibility for the withdrawals and purchases.

4. Based on the investigation by the FBI, IRS, FDIC and other law enforcement agencies, and my training and experience, I understand that the Cracking Cards bank fraud schemes generally work as follows:

**Schemers Recruit Bank Account Holders to Provide Their Debit Cards and PINs**

5. Law enforcement has obtained information about the operation of the Cracking Cards schemes from, among other sources, a Cooperating Witness. The CW has been charged by complaint in the Northern District of Illinois in relation to the CW's involvement in a Cracking Cards scheme. (The investigation in the Northern District of Illinois is related to the investigation in the Northern District of Indiana, and law enforcement has been working together on these investigations.) The CW is cooperating with law enforcement with the hope that his cooperation will be considered by the government in recommending a lower sentence. The CW has no prior criminal convictions. In addition, information provided by CW has been corroborated through witness interviews and review of financial records. I believe that the CW has provided reliable information about Cracking Card schemes.



6. According to the CW and numerous individuals who have provided their debit cards and PINs for use in the scheme, Cracking Cards schemers recruit bank account holders to give up their debit cards and PINs by promising the account holders a portion of the profits.

7. According to the CW and to individuals who were recruited to give up their debit cards, the methods of recruitment vary depending on the schemer. Some recruit card holders in person, such as at a party, at school, or on the street. Others use social media outlets such as Instagram and Facebook to advertise opportunities for making fast cash, after which account holders contact the Cracking Cards schemer by phone and listen to the schemer's pitch. Some schemers work together in pairs or groups in their recruitment efforts.

#### **Schemers Purchase or Manufacture Counterfeit Checks**

8. According to the CW, once a Cracking Cards schemer has a debit card and PIN for a third-party account, the schemer manufactures, purchases, or otherwise obtains one or more counterfeit checks to deposit into the third-party bank account. As explained by the CW and corroborated by bank records and interviews of victim businesses, the counterfeit checks used in Cracking Cards schemes generally contain legitimate bank account and routing numbers that belong to the accounts of actual business entities.<sup>1</sup>

9. According to the CW, the combination of a legitimate bank account number and routing number, as well as the name and address of the victim business, is referred to by those involved in Cracking Cards as the bank account "profile" for that business.

10. According to the CW, and as confirmed through undercover purchases of counterfeit checks from Cracking Cards schemers in Illinois, not everyone who "cracks cards"

---

<sup>1</sup> On occasion, a schemer will use a fictitious account number on a counterfeit check. Banks often float or advance the funds on a check deposit before the account number is verified and the check is cleared.

manufactures his or her own counterfeit checks to deposit into third-party accounts. Rather, certain individuals have a reputation for “making paper,” that is, making and printing counterfeit checks. The people who “make paper” sell counterfeit checks to others involved in Cracking Cards. The CW explained that he “made paper” for his own use and for selling to others who cracked cards, by using a computer software program. Participants who “make paper” obtain business profiles (bank account and routing numbers) through a variety of unauthorized and illegal means.

#### **Schemers Deposit Counterfeit Checks into Third-Party Bank Accounts**

11. According to the CW, once a Cracking Cards schemer has secured a third-party debit card and PIN, as well as one or more counterfeit checks, the schemer deposits—or recruits someone else to deposit—the counterfeit checks into the third party’s bank account, typically via an ATM transaction. As corroborated by bank records, the Cracking Cards schemer then waits for the account holder’s bank to credit the purported funds from the counterfeit check, which can happen within a matter of hours.

12. According to information provided by bank investigators, banks credit the value of a check to a card holder’s account before the check clears, that is, before the cardholder’s bank receives an image of the check (which is sent electronically to the drawer’s bank), determines whether it is valid, and requests and receives payment (or denial of payment) from the check drawer’s bank. In effect, the cardholder’s bank advances the bank’s own money into the cardholder’s account when a check is deposited—even if it is a counterfeit or fraudulent check. During the time period between the deposit of a fraudulent check and when the cardholder’s bank learns that the check is fraudulent, the advanced money in the cardholder’s bank account can be withdrawn using the cardholder’s debit card.



**Schemers Withdraw or Spend Funds from the Third-Party Bank Account**

13. According to the CW and as corroborated by bank records, after one or more counterfeit checks are deposited into a third-party bank account, the Cracking Cards schemer often attempts a relatively small ATM withdrawal (between \$100 and \$500) a few hours later, to determine whether the bank has credited the account with the purported funds from the counterfeit check. If the schemer is able to withdraw the cash at an ATM, (i.e., the bank has advanced funds to the account), the schemer goes to a point-of-sale terminal to withdraw or spend the remaining funds that the bank advanced to the third-party account because of the deposit of the counterfeit checks. Point-of-sale terminals are machines used to process debit and credit card payments, typically for the purchase of goods. For example, the machines at a grocery store checkout counter in which a customer swipes a debit card are point of sale terminals.

**Loss to Financial Institutions**

14. When floated funds are withdrawn in person at a bank branch, or at a bank ATM, as a result of a counterfeit check deposit, the bank suffers the loss when it hands the cash over to the person or dispenses it out of the machine. When floated funds are withdrawn or spent at a point-of-sale terminal, casino, or retail store, the bank suffers the loss through a series of electronic funds transfers that are managed by a debit card processing service, similar to the Automated Clearing House, but for debit transactions as opposed to credit transactions. The purchase is premised on the customer entering the correct PIN into the keypad at the store/currency exchange (the point-of-sale terminal). A communication goes from the point-of-sale terminal to the terminal's processing company, which electronically communicates with the customer's bank via the debit-processing network to verify that the PIN is accurate and that the account and its funds are accessible. At that point in the process, it is the customer's bank, via the debit-processing network, that makes the decision whether the purchase can go through. If

the bank approves the purchase, the bank is agreeing to pay back the store/currency exchange the amount of the purchase. If the purchase is approved, the store/currency exchange then hands over the product to the customer (e.g., a television or money order, or in the case of the currency exchange, cash).

15. According to the CW, Cracking Cards schemes are popular methods to obtain illicit funds and defraud banks in CC, and are carried out by numerous schemers, including those affiliated with Chicago gangs.

### **The RACK Boyz and Social Media**

16. Over the course of the investigation, the following co-conspirators were identified as part of the group that called themselves the “R.A.C.K. Boyz” or “Rack Boyz” or “TheRackBoyz”: Kevin Ford, Cortez Stevens, Stephen Garner, and Mikcale Smally (aka Mikcale Smalley). The remaining co-conspirators named herein were girlfriends of RACK Boyz and participants in the RACK Boyz Cracking Cards scheme: Mercedes Hatcher was Kevin Ford’s girlfriend, and Brittany Sims was Stephen Garner’s girlfriend. The RACK Boyz have a page on Facebook and a Twitter page. The RACK Boyz’ Facebook page has photographs posted, depicting the group members, including co-conspirators, as detailed later in this document.

17. Additionally, the RACK Boyz have videos posted on YouTube; a number of the videos on YouTube are rap videos, depicting the co-conspirators displaying large amounts of cash and featuring expensive items, such as Gucci shoes and accessories. Two such examples of their rap videos are entitled: “For the Money” and “Been Had a Bag” by the Rack Boyz. The song “For the Money” includes the lyrics “crack for the money,” referring to the Cracking Cards scheme. In the “For the Money” video, co-conspirators can be seen wearing RACK Boyz shirts and displaying large amounts of cash, as detailed later in this document.



18. “RACK Boyz” is the name for the money team that the co-conspirators are or were associated with. Money teams are groups of individuals, like the co-conspirators in this investigation, who are involved in the previously defined Cracking Cards scheme. At least one of the co-conspirators in this investigation, FORD, is now associated with a different money team, known as BandKlan. BandKlan, like the RACK Boyz, also has rap videos posted on YouTube.

19. In addition to the social media pages for the money teams, some of the co-conspirators have individual Facebook, Twitter, or Instagram pages that have been identified. On these pages, there are pictures most notably of the co-conspirators wearing t-shirts printed with the RACK Boyz money team name or displaying money and pictures of money orders and expensive cars. The co-conspirators use social media to recruit people with bank accounts or who will open bank accounts to use as Deposit Accounts in the scheme; co-conspirators sent out numerous private messages and posted messages on their walls inviting people to participate in the scheme. Information about social media accounts specific to each individual co-conspirator will be provided later in this document. The co-conspirators also identify themselves as members of the RACK Boyz on their individual Facebook pages, as detailed later in this document.

### **Co-Conspirators in the Cracking Cards Scheme**

#### **Kevin Ford**

20. Kevin Ford is an African-American male, age 26, with no known employment history or recorded wage information. Ford presently resides at 60 East Monroe, Unit 3403 in Chicago, Illinois, paying \$4,195.00 per month in rent. Information obtained through a review of postings on Kevin Ford’s Facebook page indicate that he is working as a rapper under the name Bandman Kevo and claims that he will be on tour throughout the United States and Canada during the month of October 2014; Ford’s posted tour dates match up with rapper Twista’s tour. Ford has numerous rap videos posted on YouTube as Bandman Kevo, displaying and rapping

about cash, luxury foreign cars, and expensive brands, such as Gucci. Ford appears in the aforementioned YouTube video for the RACK Boyz, "For the Money"; Ford is wearing a RACK Boyz shirt with "Kevo" printed on the back in this video.

21. Ford's Facebook profile name was "Threecarz CashedUp" and is now "BandMan Kevo." Ford also has a Twitter feed that was in the name "\$\$MASERATI KEVO\$\$," which switched to "\$\$BandMan KEVO\$\$," and is now just "BandMan KEVO." Ford also has an Instagram page, which was in the name "3CARS\_CASH" but is now in the name "BandMan Kevo." On Facebook, Twitter and Instagram, Ford posted pictures of himself wearing expensive jewelry, Gucci items, and other name-brand apparel. He posted pictures of cash, including pictures of himself counting cash. Ford has used Facebook to recruit bank account holders who have debit cards to be used in the scheme. Ford uses these photographs as a means to show his success in the scheme for which he is recruiting.

22. In addition to the cash and expensive name-brand items, Ford posted photographs on Facebook of the Maserati he previously owned, before it was seized by the government. The Maserati was seized as fruits of the crime on May 29, 2012, upon the execution of a Federal Warrant. Ford did not attempt to claim this vehicle after it was seized, and it was subsequently forfeited to the government in June 2014.

23. Ford sent out numerous private messages via Facebook as a means to recruit bank account holders. Ford sent out the same private recruiting messages as Smally, Garner and Stevens. An example of a message Ford sent out is as follows:

Yo u don't know me but we can make some cash together my brother works at citi<sup>2</sup>  
bank and he puts money on my account so I could do u a favor and have him  
put money on your account  
If u wanna make 1900 all u would have to do is open up a citi bank account n they will  
give u a temp card we would be able to do it the next day from the time u get the

---

<sup>2</sup> Ford also sent messages referencing Chase Bank instead of Citibank.



card it's 100 to open the account but if u don't got the money i will loan it too u if this is something u wanna do hit me back I will give more details  
!!! u can do this every week No BS! hit me back asap!!..  
this is no SPAM HE CAN ALSO PUT MONEY ON ANY BANK ACCOUNT!

24. Ford and co-conspirator Mercedes Hatcher have been in a relationship off and on, and they have lived together at 7116 Broadway in Merrillville, Indiana, and 60 East Monroe, Unit 3403 in Chicago, Illinois. They also have a child together. Ford also lived with co-conspirator Cortez Stevens at 7116 Broadway in Merrillville, Indiana.

25. Ford and Stevens have been seen in surveillance video depositing fraudulent checks together and purchasing money orders from a machine, using a debit card and PIN linked to an account that had fraudulent checks deposited into it. Ford and Hatcher have been seen in surveillance video purchasing money orders from a machine, using a debit card and PIN linked to an account that had fraudulent checks deposited into it. Ford has also been seen with Smally in surveillance video purchasing money orders from a machine, using a debit card and PIN linked to an account that had fraudulent checks deposited. Ford and Stevens were approached by police after purchasing money orders.

26. Ford printed fraudulent checks or "made paper," deposited fraudulent checks into third-party bank accounts, conducted withdrawals from bank accounts that had fraudulent checks deposited into them, and conducted purchases of money orders from bank accounts that had fraudulent checks deposited into them in this scheme.

**Mercedes Hatcher**

27. Mercedes Hatcher is an African-American female, age 21, with no known employment history or recorded wage information. Hatcher previously lived with Kevin Ford and Cortez Stevens at 7116 Broadway in Merrillville, Indiana. Recently, Hatcher was believed to reside with Ford at 60 East Monroe in Chicago, Illinois: bank records for Hatcher and Ford both show rent payments in the same amount to the same entity. Photographs on Facebook depict

Hatcher at this building as well. In late September 2014, Hatcher created a Facebook page for herself as an Avon sales representative.

28. Hatcher has used her cellular telephone to recruit bank account holders who have debit cards to be used in the scheme.

29. Ford and Hatcher have been seen in surveillance video purchasing money orders from a machine, using a debit card and PIN linked to an account that had fraudulent checks deposited into it. Hatcher deposited fraudulent checks into third-party bank accounts and conducted purchases of money orders from bank accounts that had fraudulent checks deposited into them in this scheme.

**Cortez Stevens**

30. Cortez Stevens is an African-American male, age 24, with no known employment history or recorded wage information since 2010. Stevens is believed to reside at 1508 North Glenwood Street, Apt. 0A in Griffith, Indiana. TheRackBoyz Facebook page has a photograph posted of Stevens wearing a RACK Boyz t-shirt; the back of the shirt reads: “#TeamR.A.C.K.”

31. Stevens’ Facebook profile name was “Cashedup Banks,” then changed to “Tez Loc” and is now “Tez Stevens.” Stevens has used Facebook to recruit bank account holders who have debit cards to be used in the scheme. Stevens sent out numerous private messages via Facebook as a means to recruit these bank account holders. Stevens sent out the same private recruiting messages as Ford, Garner and Smally. An example of a message Stevens sent out is as follows:

hey i know u don't know me but i can help you make some extra money!!! my brother works at citi bank and he puts money on my account so I could do u a favor and have him put money on your account.....If u wanna make 3000 dollars all u would have to do is open up a citi<sup>3</sup> bank account n they will give u a temp card... we would be able to do it the next day from the time u get the card it's 100 dollars to open the account but if u

---

<sup>3</sup> Stevens also sent messages referencing Bank of America instead of Citibank.



don't got the money i will loan it too u and if this is something u wanna do hit me back and I will give you more details!!! u can do this every week No BS! hit me back asap!!.. this is no SPAM HE CAN ALSO PUT MONEY ON ANY BANK ACCOUNT! think about it

32. Stevens posted photographs on Facebook of cash and expensive items, such as Air Jordan shoes and the Audi he previously owned, before it was seized by the government. The Audi was seized as fruits of the crime on May 29, 2012, upon the execution of a Federal Warrant. Stevens did not attempt to claim this vehicle after it was seized, and it was subsequently forfeited to the government in June 2014. Stevens posted the photographs of cash, shoes and the Audi as a means to show his success in the scheme for which he is recruiting.

33. Stevens and Ford have been seen together in surveillance video depositing fraudulent checks and purchasing money orders from a machine, using a debit card and PIN linked to an account that had fraudulent checks deposited into it. Stevens and Ford were approached by police after purchasing money orders. Stevens deposited fraudulent checks into third-party bank accounts, conducted withdrawals from bank accounts that had fraudulent checks deposited into them, and conducted purchases of money orders from bank accounts that had fraudulent checks deposited into them in this scheme.

#### **Stephen Garner**

34. Stephen Garner is an African-American male, age 23, with no known employment history or recorded wage information. Garner was arrested on June 11, 2014, by Portage Police Department, and he is currently being held on a warrant at Porter County Jail. At the time of his arrest, Garner had been traveling in a vehicle with the mother of co-conspirator, Brittany Sims, with whom both Garner and Sims lived. Garner and Sims have a child together.

35. Garner's Facebook profile name was "All Ways Cashin." Garner posted pictures of himself wearing Gucci accessories and with large amounts of cash coming out of his pockets. Garner uses these photographs as a means to show his success in the scheme for which he is

recruiting. Garner was pictured in group photos posted on the Facebook page with the profile name "TheRackBoyz." Garner also appears in the aforementioned YouTube video for the RACK Boyz, "For the Money." Garner is wearing a RACK Boyz shirt in the video. Garner has used Facebook to recruit bank account holders who have debit cards to be used in the scheme. Garner sent out numerous private messages via Facebook as a means to recruit these bank account holders. Garner sent out the same private recruiting messages as Ford, Smally and Stevens. An example of a message Garner sent out is as follows:

Yo u don't know me but we can make some cash together my brother works at chase bank and he puts money on my account so I could do u a favor and have him put money on your account like if he put 5,000 u keep 3,000 and give us 2,000 plus if u find me people with accounts I will give u 1,000 they don't need any money on they accounts to do this plus it could be negative!!!!IT COULD BE ANY BANK u can do this every week No BS! hit me back asap!!.....

36. Garner and Sims have been seen in surveillance footage purchasing money orders from a machine, using a debit card and PIN linked to an account that had fraudulent checks deposited into it. Garner and Smally have also been seen in surveillance footage together and were approached by police for this activity. Garner deposited fraudulent checks into third-party bank accounts, conducted withdrawals from bank accounts that had fraudulent checks deposited into them, and conducted purchases of money orders from bank accounts that had fraudulent checks deposited into them in this scheme.

#### **Brittany Sims**

37. Brittany Sims is an African-American female, age 24. Records indicate she worked for Payday Loan Store (PLS) in 2010 and 2011, and she worked at Majestic Star Casino in 2011 and 2012. Records also indicate she worked for the Board of Commissioners, with negligible wages in the fourth quarter of 2012 and first quarter of 2013. She is also known to have worked for the United States Postal Service briefly, and her employment was terminated for



reasons currently under investigation. Sims is the girlfriend of co-conspirator Stephen Garner; Sims and Garner have a child together and have lived together for years.

38. Sims and Garner have been seen together in surveillance footage purchasing money orders from a machine, using a debit card and PIN linked to an account that had fraudulent checks deposited into it.

**Mikcale Smally**

39. Mikcale Smally is an African-American male, age 21, with no known employment history or recorded wage information. On Smally's Facebook page, he listed TheRackBoyz as his job on his timeline. Smally and co-conspirator Garner have been roommates in the past.

40. Smally's Facebook profile name is "Mick Smalley (Moneymakinmick)." Smally posted pictures of what appears to be thousands of dollars in cash. Smally also posted a picture with cash piled on top of eight money orders. Smally uses these photographs as a means to show his success in the scheme for which he is recruiting. Smally posted a photograph of himself wearing a RACK Boyz shirt. On December 21, 2011, in a public post on his Facebook wall, SMALLY posted "\$\$\$\$xmas in 4 more days inbox me if you tryin make sum fast money \$\$\$\$. " Smally and Garner are pictured together in photographs on Facebook, where both have recruited bank account holders who have debit cards to be used in the scheme. Smally sent out numerous private messages via Facebook as a means to recruit these bank account holders. Smally sent out the same private recruiting messages as Ford, Garner and Stevens. An example of a message Smally sent out is as follows:

Yo u don't know me but we can make some cash together my brother works at chase bank and he puts money on my account so I could do u a favor and have him put money on your account like if he put 5,000 u keep 3,000 and give us 2,000 plus if u find me people with accounts I will give u 1,000 they don't need any money on they accounts to do this plus it could be negative!!!IT COULD BE ANY BANK u can do this every week No BS! hit me back asap!!...

41. Smally conducted purchases of money orders from impacted bank accounts in this scheme. Smally and Ford have been seen in surveillance footage purchasing money orders from a machine, using a debit card and PIN linked to an account that had fraudulent checks deposited into it. Smally and Garner have also been seen in surveillance footage conducting these transactions together and were approached by police for this activity.

### **Acts in Furtherance of the RACK Boyz Conspiracy**

#### **A. DS Account #\*\*\*\*\*867**

DS has a Chase Bank checking account (\*\*\*\*\*867). Fraudulent checks were deposited into the account by Stephen Garner. Chase deemed these checks as

The deposits in DS's account were as follows:

Date of Check	Check #	Check Payer	Drawee Bank	Check Payee	Amount	Date and Time of Deposit	Location of Deposit
08/01/2011	51891	AIC	JP Morgan Chase	CJ	\$595.23*	8/3/11 @ 4:32 p.m.	Chase Bank ATM at 1910 E. 95 <sup>th</sup> St, Chicago, IL
08/03/2011	179	DS	United States Treasury	DS	\$2,281.36	8/3/11 @ 5:01 p.m.	Chase ATM- 712 E. 87th St., Suite D2, Chicago, IL

\*The deposit amount entered at the ATM for the 4:32 p.m. deposit was \$996.23.



Video surveillance on the above deposits shows Garner<sup>4</sup> making the deposit.

The above check in the amount of \$595.23 was returned and marked as "Forgery" by Chase Bank on August 8, 2011. The other check in the amount of \$2,281.36 was returned and marked as "NSF" by Chase Bank on August 5, 2011

Below is a summary of how the proceeds of the fraudulent deposited checks were withdrawn from DS's bank account:

Date	Time	Amount	Description	Notes
8/3/2011	4:32 PM	\$200.00	Chase Bank ATM at 1910 E. 95 <sup>th</sup> St, Chicago, IL	
8/4/2011	4:01 AM	\$1,501.65	Walmart, 2400 Morthland Dr., Valparaiso, IN	Purchased 3 Money Orders \$500 with fees (.55 per MO)
8/4/2011	4:03 AM	\$956.10	Walmart, 2400 Morthland Dr., Valparaiso, IN	Purchased 2 Money Orders- \$455 and \$500 with fees (.55 per MO)
8/4/2011	5:01 AM	\$402.50	ATM W/D- 2400 Morthland Dr., Valparaiso, IN	
8/4/2011	5:02 AM	\$82.50	ATM W/D- 2400 Morthland Dr., Valparaiso, IN	

The following transactions were conducted at an MCX Machine located in the Walmart Valparaiso on August 4, 2011:

Based on video surveillance, on August 4, 2011 at 4:02 AM, Brittany Sims<sup>5</sup>, using DS's debit card and PIN, purchased three \$500 Money Gram money orders, with a \$1.65 fee, totaling \$1,501.65:

<u>Serial Number</u>	<u>Payee</u>	<u>Purchaser</u>	<u>Amount</u>
20328910304	Brittany Sims	Brittany Sims	\$500.00
20328910305	Brittany Sims	Brittany Sims	\$500.00
20328910306	Brittany Sims	Brittany Sims	\$500.00

<sup>4</sup> Investigators identified Garner in this and other instances by comparing surveillance footage with his BMV identification picture and other known pictures of Garner.

<sup>5</sup> Investigators identified Sims in this and other instances by comparing surveillance footage with her BMV identification picture and other known pictures of Sims.

At 4:04 AM, the Walmart Valparaiso video surveillance also shows Sims, using DS's debit card and PIN, purchasing an additional \$500.00 Money Gram money order and a \$445.00 Money Gram money order, with \$1.10 in fees, totaling \$956.10:

<u>Serial Number</u>	<u>Payee</u>	<u>Purchaser</u>	<u>Amount</u>
20328910307	Stephen Garner	Steve Garner	\$500.00
20328910308	Stephen Garner	MM	\$455.00

Surveillance video from Walmart Valparaiso shows Sims conducting the above transactions with Garner standing behind her. These money orders were purchased using a debit card tied to the above Chase Bank account belonging to DS.

The money orders were cashed as follows:

<u>Serial Number</u>	<u>Payee</u>	<u>Purchaser</u>	<u>Amount</u>	<u>Person who signed the back of the check</u>	<u>Notation on the Back of the Check</u>	<u>Where Cashed</u>
20328910304	Brittany Sims	Brittany Sims	\$500.00	Brittany Sims	IN 5360-01-3511	Centier Bank
20328910305	Brittany Sims	Brittany Sims	\$500.00	Brittany Sims	IN 5360-01-3511	Centier Bank
20328910306	Brittany Sims	Brittany Sims	\$500.00	B. Sims	219-779-1752	PLS Checking
20328910307	Stephen Garner	Steve Garner	\$500.00	Stephen Garner	773-596-4980	PLS Checking
20328910308	Stephen Garner	MM	\$455.00	Stephen Garner	773-596-4980	PLS Checking

The backs of the checks reflected a bank cleared date of 8/5/11. The Indiana ID number that was on Brittany Sims' checks is her ID number. The phone numbers listed are associated with Sims and Garner.

## **B. YH Account #\*\*\*\*\*488**

YH had a checking account (\*\*\*\*\*488) at Chase Bank.



On August 5, 2011, the following fraudulent deposits were made into YH's checking account (\*\*\*\*\*488):

Date of Check	Check #	Check Payer	Drawee Bank	Check Payee	Amount	Date and Time of Deposit	Location of Deposit
08/03/11	5326	VP	JPMorgan Chase	YH	\$1,596.21	08/05/11 at 4:17 PM	Chase ATM, 10440 S. Cicero Avenue, Oak Lawn, IL
08/03/11	5323	VP	JPMorgan Chase	YH	\$1,423.53	08/05/11 at 4:18 PM	Chase ATM, 10440 S. Cicero Avenue, Oak Lawn, IL
Total					\$3,019.74		

Video surveillance from Chase shows a dark-skinned arm coming out of the window of a silver Audi sedan making the deposits, using a debit card and PIN; the license plate is not visible on surveillance coverage. Ford drove a silver Audi sedan at this time<sup>6</sup>. He also was seen in the Audi making fraudulent deposits in other legitimate accounts in the scheme.

Both of the above deposited checks were returned and marked as "Altered Fictitious" by Chase Bank on August 9, 2011.

Below is a summary of how the proceeds of the fraudulent deposited checks were withdrawn from YH's bank account:

Date	Time	Amount	Description	Notes
8/5/2011	4:19 AM	\$200.00	Chase ATM W/D, 10440 S. Cicero Avenue, Oak Lawn, IL	
8/6/2011	5:56 AM	\$1,501.65	Walmart, Valparaiso, IN	Purchased 3 Money Orders \$500 with fees (.55 per MO)
Total		\$1,701.65		

The money orders that were purchased from the above withdrawal are summarized below:

Money Order #	Payee	Purchaser	Amount	Date Purchased	Time Purchased	Purchased From	Notes
20328910361	Mikcale Smalley	(illegible)	\$500.00	8/6/2011	5:57 AM	Walmart-Valparaiso	On the back of the check-4987 Georgia; this address had been used by several of the people involved in this

<sup>6</sup> On 8/18/2011 video surveillance footage from fraudulent ATM transactions depict a silver Audi sedan, bearing a license plate that comes back to Kevin Ford, and the driver of the silver Audi in this footage appears to be Kevin Ford (see RA's section later in this document).

							scheme
20328910362	CD	JB	\$500.00	8/6/2011	5:57 AM	Walmart-Valparaiso	9817 S. Forest
20328910363	MM	AW	\$500.00	8/6/2011	5:57 AM	Walmart-Valparaiso	On the back of the check-312-802-5234; phone number associated with MM

Video surveillance from the MCX machine located in the Walmart, Valparaiso, IN on 8/6/11 shows Kevin Ford and Mercedes Hatcher<sup>7</sup> purchasing the above money orders, using a debit card and PIN.

YH told agents that she was incarcerated at the time that the checks were deposited and the funds were withdrawn. She had left her personal belongings, which included her debit card, at a friend's house when she went to jail. YH does not know any of the above named individuals, nor did she give anyone permission to use her debit card.

### C. DG Account #\*\*\*\*\*997

DG had a Citibank checking account (\*\*\*\*\*997). DG stated that MM had paid him \$500.00 (in the form of a money order, which was purchased with DG's debit card) for his debit card and PIN.

DG's Citibank checking account (\*\*\*\*\*997) had five fraudulent checks deposited into it; all of the fraudulent checks appeared to be business checks for AGPC. These fraudulent AGPC checks had the same digital signature on them that was used on many of the fraudulent checks deposited in this scheme. The image of this signature was found on the computer at the apartment shared by Kevin Ford, Cortez Stevens, and Mercedes Hatcher. The payer (AGPC) has been used on other fraudulent checks that were used in this scheme.

The deposits in DG's Citibank checking account (\*\*\*\*\*997) were as follows:

Date of Check	Check #	Check Payer	Drawee Bank	Check Payee	Amount	Date and Time of Deposit	Location of Deposit
08/04/2011	1186623	AGPC	d States Treasurer/Financial Mgt	DG	\$3,728.64	8/4/11 @ 1:33 p.m.	Citibank, 5812 S. Ellis Ave., Chicago, IL
08/05/2011	1186624	AGPC	d States Treasurer/Financial Mgt	DG	\$4,763.92	8/5/11 @ 1:05 p.m.	Citibank, 8650 S. Stony

<sup>7</sup> Investigators identified Ford and Hatcher in this and other instances by comparing surveillance footage with their BMV identification pictures and other known pictures of Ford and Hatcher. Investigators have also met with and spoken to Ford and Hatcher in person.



							Island, Chicago, IL
08/08/2011	1186630	AGPC	United States Treasurer	DG	\$5,263.91	8/8/11 @ 10:38 a.m.	Citibank, 8650 S. Stoney Island, Chicago, IL
08/09/2011	1186638	AGPC	United States Treasurer	DG	\$6,342.68*	8/9/11 @ 11:46 a.m.	Citibank, 8650 S. Stoney Island, Chicago, IL
08/10/2011	1186652	AGPC	United States Treasurer	DG	\$5,681.37	8/10/11 @ 11:47 a.m.	Citibank, 8650 S. Stoney Island, Chicago, IL
Total					\$25,780.52		

\* The bank statement reflects a deposit of \$6,842.68.

Video surveillance from Citibank for 8/9/11 and 8/10/11 show MM depositing the above fraudulent checks into DG's account, using a debit card and PIN.

The above checks were all returned as unpaid. They were deemed unpaid by Citibank on the following dates:

Check #	Check Amount	Date Deemed Unpaid
1186623	\$3,728.64	08/11/2011
1186624	\$4,763.92	08/12/2011
1186630	\$5,263.91	08/15/2011
1186638	\$6,342.68*	08/16/2011
1186652	\$5,681.37	08/17/2011

**Information for the August 4, 2011 \$3,728.64 check deposited**

The funds for August 4, 2011 check for \$3,728.64 was withdrawn/spent as follows:

Date	Time	Amount	Description
08/04/2011	1:34 PM	\$300.00	Citibank ATM, 5812 S. Ellis, Chicago, IL
08/05/2011	6:41 AM	\$1,000.00	Citibank ATM, 8650 S. Stoney Island, Chatham, IL

08/05/2011	7:47 AM	\$2,002.20	MCX- Walmart, Valparaiso, IN
08/05/2011	7:50 AM	\$400.55	MCX- Walmart, Valparaiso, IN
Total		\$3,702.75	

No video surveillance was available for the above transactions.

Money orders purchased at the MCX machine in Walmart for the above-listed MCX Walmart transactions are as follows:

Money Order #	Payee	Purchaser	Amount	Date Purchased	Time Purchased	Notes
20328910319	MM	AW	\$500.00	8/5/11	7:49 AM	312-802-5234
20328910320	MM	AW	\$500.00	8/5/11	7:49 AM	312-802-5234
20328910321	MM	AW	\$500.00	8/5/11	7:49 AM	312-802-5234
20328910322	DG	HW	\$500.00	8/5/11	7:49 AM	
20328910323	Mikcale Smalley	Mikcale Smalley	\$400.00	8/5/11	7:51 AM	773-639-7801 or 7851?
Total			\$2,400.00			

**Information for the August 5, 2011 \$4,763.92 check deposited**

The funds for the August 5, 2011 deposit of \$4,763.92 were withdrawn/spent as follows:

Date	Time	Amount	Description
08/06/2011	8:07 AM	\$71.25	Speedway, Hobart, IN
08/06/2011	9:20 AM	\$30.00	4717 W. 61st Avenue, Hobart, IN
08/06/2011	2:28 PM	\$100.00	Citibank ATM, 8650 S. Stoney Island, Chatham, IL
08/06/2011	2:29 PM	\$100.00	Citibank ATM, 8650 S. Stoney Island, Chatham, IL
08/07/2011	7:19 PM	\$1.09	1497 Wal-Sams, Matteson, IL
08/08/2011	6:47 AM	\$500.00	Citibank ATM, 8650 S. Stoney Island, Chatham, IL
08/08/2011	6:55 AM	\$200.00	Citibank ATM, 8650 S. Stoney Island, Chatham, IL
08/08/2011	6:56 AM	\$100.00	Citibank ATM, 8650 S. Stoney Island, Chatham, IL
08/08/2011	8:05 AM	\$2,002.20	MCX- Walmart, Valparaiso, IN
08/08/2011	8:08 AM	\$1,602.20	MCX- Walmart, Valparaiso, IN
08/08/2011	8:17 AM	\$45.06	Speedway, Valparaiso, IN
Total		\$4,751.80	



Money orders purchased in Walmart for the above-listed MCX Walmart transactions are as follows:

Money Order #	Payee	Purchaser	Amount	Date Purchased	Time Purchased	Notes
20328910376	DR	MP	\$500.00	8/8/11	8:06 AM	ID IL ***-1100
20328910377	TW	HM	\$500.00	8/8/11	8:06 AM	***-**-1619
20328910378	TJ	CJ	\$500.00	8/8/11	8:06 AM	312-545-5592
20328910379	MM	AW	\$500.00	8/8/11	8:06 AM	312-802-5234
20328910380	MM	AW	\$500.00	8/8/11	8:09 AM	***-**-6754
20328910381	MM	AW	\$500.00	8/8/11	8:09 AM	312-802-5234
20328910382	TH	AW	\$300.00	8/8/11	8:09 AM	***-**-3946; 773-979-2166
20328910383	TH	AW	\$300.00	8/8/11	8:09 AM	***-**-3946
Total			\$3,600.00			

Video surveillance from the MCX machine located in the Walmart, Valparaiso, IN on 8/8/11 show Kevin Ford withdrawing the money orders, using a debit card and PIN.

**Information for the August 8, 2011 \$5,263.91 check deposited**

The funds for the August 8, 2011 deposit of \$5,263.91 were withdrawn:

Date	Time	Amount	Description
08/09/2011	6:19 AM	\$500.00	Citibank ATM, 8650 S. Stoney Island, Chatham, IL
08/09/2011	6:19 AM	\$500.00	Citibank ATM, 8650 S. Stoney Island, Chatham, IL
08/09/2011	7:26 AM	\$2,002.20	MCX- Walmart, Valparaiso, IN
08/09/2011	7:29 AM	\$2,002.20	MCX- Walmart, Valparaiso, IN
08/09/2011	7:32 AM	\$294.55	MCX- Walmart, Valparaiso, IN
Total		\$5,298.95	

Money orders purchased at the MCX machine in Walmart on the above dates are as follows:

Money Order #	Payee	Purchaser	Amount	Date Purchased	Time Purchased	Notes
20328910398	MM	AW	\$500.00	8/9/11	7:27 AM	312-802-5234
20328910399	MM	AW	\$500.00	8/9/11	7:27 AM	312-802-5234
20328910400	MM	AW	\$500.00	8/9/11	7:27 AM	312-802-5234

20328910401	MM	AW	\$500.00	8/9/11	7:27 AM	312-802-5234
20328910402	TJ	DS	\$500.00	8/9/11	7:30 AM	
20328910403	GC	DB	\$500.00	8/9/11	7:30 AM	
20328910404	TW	LB	\$500.00	8/9/11	7:30 AM	
20328910405	JJ	DT	\$500.00	8/9/11	7:30 AM	
20328910406	VM	VM	\$294.00	8/9/11	7:33 AM	Cashed at New Dolton Currency
Total			\$4,294.00			

Video surveillance from the MCX machine located in the Walmart, Valparaiso, IN on 8/9/11 show Kevin Ford withdrawing the money orders, using a debit card and PIN.

VM is the girlfriend of Cortez Stevens.

**Information for the August 9, 2011 \$6,342.68 check deposited**

The funds for the August 9, 2011 deposit of \$6,342.68 were withdrawn:

Date	Time	Amount	Description
08/10/2011	6:12 AM	\$1,000.00	Citibank ATM, 8650 S. Stoney Island, Chatham, IL
08/10/2011	7:16 AM	\$2,002.20	MCX- Walmart, Valparaiso, IN
08/10/2011	7:19 AM	\$2,002.20	MCX- Walmart, Valparaiso, IN
08/10/2011	7:40 AM	\$851.10	MCX- Walmart, Valparaiso, IN
Total		\$5,855.50	

Money orders purchased at the MCX machine in Walmart on the above dates are as follows:

Money Order #	Payee	Purchaser	Amount	Date Purchased	Time Purchased	Notes
20328910411	TH	AW	\$500.00	8/10/11	7:17 AM	***-**-3846
20328910412	MM	AW	\$500.00	8/10/11	7:17 AM	312-802-5234
20328910413	MM	AW	\$500.00	8/10/11	7:17 AM	312-802-5234
20328910414	MM	AW	\$500.00	8/10/11	7:17 AM	312-802-5234
20328910415	MM	AW	\$500.00	8/10/11	7:20 AM	312-802-5234
20328910416	MM	AW	\$500.00	8/10/11	7:20 AM	312-802-5234
20328910417	MM	AW	\$500.00	8/10/11	7:20 AM	312-802-5234
20328910418	MM	AW	\$500.00	8/10/11	7:20 AM	312-802-5234
20328910419	TH	AW	\$500.00	8/10/11	7:41 AM	***-**-3946
20328910420	TH	AW	\$350.00	8/10/11	7:41 AM	***-**-3946
Total			\$5,850.00			



Video surveillance from the MCX machine located in the Walmart, Valparaiso, IN on 8/10/11 shows Kevin Ford purchasing the money orders, using a debit card and PIN.

Funds for the 08/10/11 check (\$5,681.37) were not accessed based on this deposit since the previous checks were coming back as unpaid and fraudulent.

#### **D. BM Account #\*\*\*\*\*227**

BM had a checking account (\*\*\*\*\*227) at Citibank. BM stated that Cortez Stevens had stolen her Citibank debit card and PIN. She left her purse in Steven's car when he stole the information. BM also stated that Stevens bragged on Facebook about what he had done to her. She also filed a police report on August 11, 2011, regarding the theft with Chicago PD (report HT443233).

The deposits in BM's Citibank checking account (\*\*\*\*\*227) were as follows:

Date of Check	Check #	Check Payer	Drawee Bank	Check Payee	Amount	Date and Time of Deposit	Location of Deposit
08/08/2011	1186629	AGPC	United States Treasurer	BM	\$4,388.26	8/8/11 @ 11:44 AM	Citibank, 1779 River Oaks Drive, Calumet City, IL
08/08/2011	753	JW	First Midwest Bank	BM	\$4,213.32	8/8/11 @ 1:46 PM	Citibank, 1779 River Oaks Drive, Calumet City, IL
08/09/2011	1186637	AGPC	United States Treasurer	BM	\$4,261.90	8/9/11 @ 10:23 AM	Citibank, 1779 River Oaks Drive, Calumet City, IL
08/10/2011	1186653	AGPC	United States Treasurer	BM	\$5,211.90	8/10/11 @ 12:45 PM	Citibank, 1779 River Oaks Drive, Calumet City, IL
Total					\$18,075.38		

Cortez Stevens<sup>8</sup> can be seen in Citibank bank surveillance video conducting the following two fraudulent deposits into BM's Citibank account on August 9, 2011 and August 10, 2011, using a debit card and PIN. There was no video surveillance available for the deposits on August 8, 2011.

The fraudulent checks appeared to be business checks for AGPC, just like the ones deposited into the account for DG. Again, these fraudulent AGPC checks had the same digital signature on them that was used on many of the fraudulent checks deposited in this scheme. The image of the payer on the AGPC checks signature was found during a search warrant on the computer at Cortez Stevens, Mercedes Hatcher, and Kevin Ford's apartment.

The above checks were all returned as unpaid. They were deemed unpaid by Citibank on the following dates:

Check #	Check Amount	Date Deemed Unpaid
1186629	\$4,388.26	08/15/2011
753	\$4,213.32	08/11/2011
1186637	\$4,261.90	08/16/2011
1186653	\$5,211.90	08/17/2011

Below is a summary of how the proceeds of the fraudulent deposited checks were withdrawn from BM's bank account:

Date	Time	Amount	Description	Notes
8/8/2011	11:47 AM	\$800.00	Citibank ATM, 1779 River Oaks Dr, Calumet City, IL	
8/8/2011	11:57 AM	\$1,001.20	Walmart-Lansing, IL	Purchased 1 Money Order \$1,000 with fee (.60) and had \$500.60 returned as cash
8/8/2011	12:30 PM	\$2,001.10	Walmart, Hammond, IN	Purchased 2 Money Orders \$1, 000 with fees (.55 per MO)
8/8/2011	12:32 PM	\$354.64	Walmart, Hammond, IN	Purchased 1 Money Pak \$350 with fee of \$4.64
8/8/2011	1:47 PM	\$40.00	Citibank ATM, 1779 River Oaks Dr, Calumet City, IL	
8/9/2011	7:05 AM	\$183.00	Non-Citibank ATM, 4001 W. 167th St, Country Club, IL (Chase)	
8/9/2011	11:13 AM	\$803.00	Non-Citibank ATM, 7 Sibley Rd, Hammond, IN (Walgreens)	
8/9/2011	11:26 AM	\$2,001.10	Walmart, Hammond, IN	Purchased 2 Money Orders \$1, 000 with fees (.55 per MO)

<sup>8</sup> Investigators identified Stevens in this and other instances by comparing surveillance footage with his BMV identification picture and other known pictures of Stevens.



8/9/2011	11:30 AM	\$1,004.64	Walmart, Hammond, IN	Purchased 1 Money Pak \$1000 with fee of \$4.64
8/9/2011	3:39 PM	\$10.89	Lansing Square, 16756 Torrence Ave, Lansing, IL	Debit PIN purchase
8/9/2011	3:41 PM	\$10.89	Lansing Square, 16756 Torrence Ave, Lansing, IL	Debit PIN purchase
8/9/2011	4:00 PM	\$52.77	Walmart, Lansing, IL	Misc items purchased
8/10/2011	6:56 AM	\$503.00	Chase Bank, Country Club Hills, IL	
8/10/2011	7:24 AM	\$1,004.64	Walmart, Lansing, IL	Purchased 1 Money Pak \$1000 with fee of \$4.64 (On stmt as 8/11/11)
8/10/2011	7:24 AM	\$1,004.64	Walmart, Lansing, IL	Purchased 1 Money Pak \$1000 with fee of \$4.64 (On stmt as 8/11/11)
8/10/2011	7:40 AM	\$403.00	Walgreens, 6510 Columbia, Hammond, IN	
8/10/2011	7:45 AM	\$1,501.10	Walmart, Hammond, IN	Purchased 2 Money Orders \$1,000 and \$500 with fees (.55 per MO) (On stmt as 8/11/11)
8/10/2011	12:33 PM	\$185.00	Connection Wear, Calumet City, IL	
8/10/2011	12:45 PM	\$580.00	Citibank ATM, 1779 River Oaks Dr, Calumet City, IL	

Video surveillance from Walmart at 165<sup>th</sup> Street in Hammond from August 9, 2011 shows Cortez Stevens at the Money Center counter at 11:26 AM, using a debit card. Surveillance also shows Stevens at a cash register checking out at 11:29 AM.

The money orders that were purchased from the above withdrawals are summarized below:

Money Order #	Payee	Purchaser	Amount	Date Purchased	Time Purchased	Purchased From	Notes
20320807175			\$500.00	8/8/2011	11:57 AM	Walmart-Lansing	
20335481106	Cortez Stevens	Blank	\$1,000.00	8/8/2011	12:31 PM	Walmart-Hammond	Cashed at New Dolton Currency
20335481107	Cortez Stevens	Blank	\$1,000.00	8/8/2011	12:31 PM	Walmart-Hammond	Cashed at New Dolton Currency
20335480663	Blank	Cortez Stevens	\$1,000.00	8/9/2011	11:27 AM	Walmart-Hammond	Cashed at New Dolton Currency
20335480664	Blank	Cortez Stevens	\$1,000.00	8/9/2011	11:27 AM	Walmart-Hammond	Cashed at New Dolton Currency
20335481132	Blank	Cortez Stevens	\$1,000.00	8/10/2011	7:46 AM	Walmart-Hammond	Cashed at New Dolton Currency

20335481133	Cortez Stevens	Cortez Stevens	\$500.00	8/10/2011	7:46 AM	Walmart- Hammond	Cashed at New Dolton Currency
-------------	-------------------	-------------------	----------	-----------	---------	---------------------	----------------------------------

The GE Money Pak cards that were purchased from the above withdrawals are summarized below:

Money Pak #	Amount	Date Purchased	Time Purchased	Purchased From
06298108401924	\$350.00	8/8/2011	12:32 PM	Walmart, Hammond, IN
28314489938515	\$1,000.00	8/9/2011	11:30 AM	Walmart, Hammond, IN
68761402466387	\$1,000.00	8/10/2011	7:24 AM	Walmart, Lansing, IL
58099161220852	\$1,000.00	8/10/2011	7:25 AM	Walmart, Lansing, IL

### E. LB Account #\*\*\*\*\*123

LB had a checking account (\*\*\*\*\*123) at Bank of America.

LB stated that Stephen Garner recruited her for the scheme, paying her \$1,000.00 to give him her debit card and PIN. After LB gave her debit card and PIN to Garner, a fraudulent check was deposited into her account at the Bank of America ATM located at 83<sup>rd</sup> and Princet, Chicago, IL on August 12, 2011. The deposit is detailed below:

Date of Check	Check #	Check Payer	Drawee Bank	Check Payee	Amount	Date of Deposit	Location of Deposit
08/12/2011	5483	NHKKH	Bank of America	LB	\$1,876.89	08/12/2011	Bank of America ATM, 83rd and Princet, Chicago, IL

Below is a summary of how the proceeds of the fraudulent deposited check were withdrawn from LB's bank account:

Date	Amount	Description	Notes
8/12/2011	\$160.00	Bank of America ATM W/D, 83rd & Princet, Chicago, IL	
8/13/2011	\$1,501.65	Walmart, Valparaiso, IN	Purchased 3 Money Orders \$500 with fees (.55 per MO)
8/13/2011	\$182.50	Withdrawal, 2400 Morthland, Valparaiso, IN	ATM in Walmart
Total	\$1,844.15		

The money orders that were purchased from the above withdrawal are summarized below:

Money Order #	Payee	Purchaser	Amount	Date Purchased	Time Purchased	Purchased From	Notes
---------------	-------	-----------	--------	-------------------	-------------------	-------------------	-------



20328910450	B Sims	B Sims	\$500.00	8/13/2011	5:11 AM	Walmart-Valparaiso	Notation on the check: 219-779-1752; 5802 Adams St. (This is Sims phone number and address)
20328910451	LB	Stephen Garner	\$500.00	8/13/2011	5:11 AM	Walmart-Valparaiso	LB's Fee for giving the card and PIN to Garner
20328910452	LB	Stephen Garner	\$500.00	8/13/2011	5:11 AM	Walmart-Valparaiso	LB's Fee for giving the card and PIN to Garner

Video surveillance from the MCX machine located in the Walmart, Valparaiso, IN on 8/13/11 shows Stephen Garner purchasing the above money orders, using a debit card and PIN.

The two money orders that were in the name of LB were given to LB by Garner for payment for the use of her debit card and PIN in the scheme.

#### **F. RA Account #\*\*\*\*\*306**

RA had a checking account (\*\*\*\*\*306) with Chase Bank.

On August 18, 2011, three fraudulent checks were deposited into the account (\*\*\*\*\*306) of RA. The deposited checks are detailed below:

Date of Check	Check #	Check Payer	Drawee Bank	Check Payee	Amount	Date and Time of Deposit	Location of Deposit
08/18/2011	216971	AAAHAC	JPMorgan Chase	RA	\$1,509.22	08/18/2011 at 8:15 PM	Chase ATM, 16767 Torrence Avenue, Lansing, IL
08/18/2011	216965	AAAHAC	JPMorgan Chase	RA	\$1,909.22	08/18/2011 at 8:15 PM	Chase ATM, 16767 Torrence Avenue, Lansing, IL
08/18/2011	216968	AAAHAC	JPMorgan Chase	RA	\$1,990.22	08/18/2011 at 8:16 PM	Chase ATM, 16767 Torrence Avenue, Lansing, IL
					\$5,408.66		

Video surveillance shows Kevin Ford depositing the above check into RA's account, using a debit card and PIN. Seconds later, surveillance video shows Ford making an ATM withdrawal on RA's account. The video surveillance images shows a silver Audi, Indiana license plate SP 5306 parked at the drive-up

ATM machine from which the deposits were made into RA's bank account. Indiana License plate SP 5306 traces back to a Cadillac owned by Kevin Ford.

All three of the above deposited checks were returned and marked as "Altered Fictious" by Chase Bank on August 22, 2011.

Below is a summary of how the proceeds of the fraudulent deposited checks were withdrawn from RA's bank account:

Date	Time	Amount	Description	Notes
08/18/2011	8:16 PM	\$100.00	ATM W/D, 16767 Torrence Ave, Lansing, IL	
08/19/2011	5:43 AM	\$1,501.65	Walmart, Valparaiso, IN	Purchased 3 Money Orders \$500 with fees (.55 per MO)
08/19/2011	6:44 AM	\$482.50	ATM W/D, 2400 Morthland Dr., Valparaiso, IN	ATM inside Walmart
Total		\$2,084.15		

The money orders that were purchased from the above withdrawals are summarized below:

Money Order #	Payee	Purchaser	Amount	Date Purchased	Time Purchased	Purchased From	Notes
20340982534	Kevin Ford	Kevin Ford	\$500.00	08/19/2011	5:45 AM	Walmart-Valparaiso	On the back of the check-260-267-4944
20340982535	AJ	HJ	\$500.00	08/19/2011	5:45 AM	Walmart-Valparaiso	10839 Wentworth
20340982536	KM	KM	\$500.00	08/19/2011	5:45 AM	Walmart-Valparaiso	On the back of the check-708-527-6480

There was an attempt to purchase four money orders with fees (\$2,002.20) at Walmart, Valparaiso, IN at 5:46 AM. The purchase was declined.

On the above-listed money order for KM, the address 700 Greenbay Avenue was listed; on law enforcement database checks, Kevin Ford is also associated with this address (700 Greenbay Ave., Calumet City, IL), for utility listings. KM's name appears on other money orders that were purchased with funds from fraudulent checks that were deposited in this scheme.

Video surveillance from the MCX machine located in the Walmart, Valparaiso, IN on 8/19/11 shows Kevin Ford purchasing the above money orders, using a debit card and PIN.



On August 19, 2011, Walmart had contacted the Valparaiso Police, who responded at 5:51 AM, reporting two suspicious black males who keep entering the store attempting to use the ATM and money order machines. A police report was filed.

RA was interviewed in March 2012 regarding this Chase Bank account. He claimed that his debit card had been stolen from him. RA did volunteer, however, that he had been approached by people who wanted to use his debit card to allow money to be transferred to his account. RA claimed that he did not engage in this behavior.

### **G. LM Account #\*\*\*\*\*581**

LM opened a checking account (\*\*\*\*\*581) at US Bank on June 14, 2011 with a deposit of \$50.

On August 29, 2011, a fraudulent check was deposited into the US Bank checking account (\*\*\*\*\*581) of LM at an US Bank ATM located at the East Side, Chicago, IL. The deposited check is detailed below:

Date of Check	Check #	Check Payer	Drawee Bank	Check Payee	Amount	Date and Time of Deposit	Location of Deposit
08/29/2011	10690	SC	JPMorgan Chase	LM	\$2,481.06	08/29/2011, 4:49 PM	US Bank ATM, East Side, Chicago, IL

The signature of the payer is the same signature that has appeared on other fraudulent checks in this scheme. A digital copy of the signature was also found on the computer located at Kevin Ford, Mercedes Hatcher, and Cortez Stevens' apartment during a search warrant.

US Bank marked the above deposited check as "deposited item returned" on September 6, 2011.

Below is a summary of how the proceeds of the fraudulent deposited checks were withdrawn from LM's bank account:

Date	Amount	Description	Notes
8/29/2011	\$60.00	US Bank ATM W/D, East Side, Chicago, IL	
8/30/2011	\$95.55	Walmart, Valparaiso, IN	Purchased 1 Money Order \$95 with fees (.55 per MO)
8/30/2011	\$400.55	Walmart, Valparaiso, IN	Purchased 1 Money Order \$400 with fees (.55 per MO)
8/30/2011	\$482.50	ATM W/D, 2400 Morthland Drive, Valparaiso, IN	Inside Walmart
8/30/2011	\$500.55	Walmart, Valparaiso, IN	Purchased 1 Money Order \$500 with fees (.55 per MO)
Total	\$1,539.15		

The money orders that were purchased from the above withdrawal are summarized below:

Money Order #	Payee	Purchaser	Amount	Date Purchased	Time Purchased	Purchased From	Notes
20340982673	CD	LB	\$500.00	8/30/2011	4:32 AM	Walmart-Valparaiso	300 W. 105 <sup>th</sup> Street, Chicago, IL
20340982674	CD	LB	\$400.00	8/30/2011	4:37 AM	Walmart-Valparaiso	300 W. 105 <sup>th</sup> Street, Chicago, IL
20340982675	Unknown	Unknown	\$95.00	8/30/2011	4:39 AM	Walmart-Valparaiso	

Video surveillance from the MCX machine located in the Walmart, Valparaiso, IN on 8/30/11 shows Mikcale Smally<sup>9</sup> and Stephen Garner at the machine from at least 4:32 AM until 4:34 AM. Both are conducting transactions with debit cards and PINs from this machine during that time, and both are present to purchase the money orders from LM's account.

On that date at 4:32 AM, Walmart called Valparaiso Police to report suspicious behavior. Later when police arrived, LW, CT, and Stephen Garner were sitting in a vehicle. They stated that their friend (Mikcale Smally) was inside purchasing a video game. Police located Smally inside Walmart. The police later learned that all four individuals had been inside Walmart and there had been \$3,000 in cash withdrawals made from the ATM located inside Walmart. CT had \$1,100 in money orders and \$190 in cash on his possession. Garner had \$400 in cash on his possession.

On September 6, 2011, LM filed a claim with US Bank that stated that she lost her debit card.

LM told agents that her card was stolen, and she did not deposit the above mentioned checks into her bank account. She also stated that she did not know Mikcale Smally.

## **H. CP Account #\*\*\*\*\*475**

On December 19, 2011, CP opened a Citibank checking account #\*\*\*\*\*475. \$100 USC was used for the initial deposit.

On December 20, 2011, the following fraudulent deposit was made into CP's account:

Date of Check	Check #	Check Payer	Drawee Bank	Check Payee	Amount	Date and Time of Deposit	Location of Deposit

<sup>9</sup> Investigators identified Smally in this and other instances by comparing surveillance footage with his BMV identification picture and other known pictures of Smally.



12/20/11	217696	CC	State Treasurer of Illinois	CP	\$3,991.17	12/20/11 at 10:41 AM	Citibank #90, 17401 S. Oak Park, Tinley Park, IL
----------	--------	----	-----------------------------------	----	------------	-------------------------	---

The image of the payee's signature was found on the computer that was located in Cortez Stevens, Mercedes Hatcher, and Kevin Ford's apartment during a search warrant. The signature also appears on other fraudulent checks that Stevens and Ford used in the scheme. The payer (CC) and the drawee bank (State Treasurer of Illinois) have been listed on other fraudulent checks that are a part of this scheme.

Video surveillance shows Cortez Stevens depositing the above check into CP's account, using a debit card and PIN. Seconds later, surveillance video shows Stevens making an ATM withdrawal on CP's account.

The above check was returned and deemed unpaid by Citibank on December 22, 2012.

Below is a summary of how the proceeds of the fraudulent deposited check were withdrawn from CP's bank account:

Date	Time	Amount	Description
12/20/2011	10:42 AM	\$340.00	Citibank ATM Withdrawal, 17401 S. Oak Park, Tinley Park, IL
12/21/2011	4:47 AM	\$500.60	Walmart, Belvidere, IL
12/21/2011	4:48 AM	\$2,002.40	Walmart, Belvidere, IL
12/21/2011	4:51 AM	\$1,201.80	Walmart, Belvidere, IL

### **I. TS Account #\*\*\*\*\*533**

On January 20, 2012, TS opened a Citibank checking account (\*\*\*\*\*533) and a savings account (\*\*\*\*\*541) and funded each account with \$50.00 USC. She had a debit card for the above mentioned accounts.

TS's Citibank checking and savings account had three fraudulent checks deposited into them. The fraudulent checks had a digital signature on them that was used on many of the fraudulent checks deposited in this scheme. The image of this signature was found on the computer at the apartment shared by Kevin Ford, Cortez Stevens, and Mercedes Hatcher.

Recent attempts to find updated contact information for TS have been unsuccessful.

The deposits in TS's checking account (\*\*\*\*\*533) were as follows:

Date of Check	Check #	Check Payer	Drawee Bank	Check Payee	Amount	Date and Time of Deposit	Location of Deposit
02/22/2012	10101	CC	State Treasurer of Illinois	TS	\$3,999.85	2/22/12 @ 11:45 a.m.	Citibank, 1779 River Oaks Dr., Calumet City, IL
02/21/2012	138	CC	PNC Bank	RS	\$3,999.39	2/23/12 @ 6:47 a.m.	Citibank, 1779 River Oaks Dr., Calumet City, IL
Total					\$7,999.24		

The deposit in TS's savings account (\*\*\*\*\*541) was as follows:

Date of Check	Check #	Check Payer	Drawee Bank	Check Payee	Amount	Date and Time of Deposit	Location of Deposit
02/21/2012	140	CC	PNC Bank	RM	\$1,492.35	2/23/12 @ 6:49 a.m.	Citibank, 1779 River Oaks Dr., Calumet City, IL

A total of \$9,491.59 of fraudulent checks was deposited into TS's bank accounts.

Video surveillance film was not available for the above deposits.

The above checks were all returned as unpaid. They were deemed unpaid by Citibank on the following dates:

Check #	Check Amount	Date Deemed Unpaid
10101	\$3,999.85	02/28/2012
138	\$3,999.39	02/24/2012
140	\$1,492.35	02/27/2012



Prior to the bank realizing that the deposited checks were fraudulent, the following transactions were conducted from TS's checking account (\*\*\*\*\*533):

Date	Time	Amount	Description
02/22/2012	11:46 AM	\$260.00	Citibank ATM Cash Withdrawal, 1779 River Oaks Dr., Calumet City, IL
02/23/2012	4:20 AM	\$2,002.40	1978 Wal-Sams (Walmart), Plymouth, IN
02/23/2012	4:20 AM	\$1,702.40	1978 Wal-Sams (Walmart), Plymouth, IN
02/23/2012	4:25 AM	\$22.50	2505 N. Oak Rd., Plymouth, IN
02/23/2012	6:48 AM	\$280.00	Citibank ATM Cash Withdrawal, 1779 River Oaks Dr., Calumet City, IL
Total		\$4,267.30	

The following transactions were conducted from TS's savings account (\*\*\*\*\*541):

Date	Time	Amount	Description
02/23/2012	unknown	\$200.00	Citibank ATM Cash Withdrawal, 1779 River Oaks Dr., Calumet City, IL

Money orders purchased at Walmart in Plymouth, Indiana for the above-listed Walmart transactions are as follows:

Money Order #	Payee	Purchaser	Amount	Date Purchased	Time Purchased	Notes
20361157840	KM	KM	\$500.00	02/23/12	05:19 AM (EST)	708-527-6980
20361157841	KM	KM	\$500.00	02/23/12	05:19 AM (EST)	708-527-6980
20361157842	KM	KM	\$500.00	02/23/12	05:19 AM (EST)	708-527-6980
20361157843	KM	KM	\$500.00	02/23/12	05:19 AM (EST)	708-527-6980
20361157844	KM	KM	\$500.00	02/23/12	05:22 AM (EST)	708-527-6980
20361157845	KM	KM	\$500.00	02/23/12	05:22 AM (EST)	708-527-6980
20361157846	Cortez Stevens	Cortez Stevens	\$500.00	02/23/12	05:22 AM (EST)	708-600-6450
20361157847	Cortez Stevens	Cortez Stevens	\$200.00	02/23/12	05:22 AM (EST)	708-600-6450
Total			\$3,700.00			

Walmart video surveillance shows both Ford and Stevens at the MCX conducting transactions, using a debit card and PIN.

On February 23, 2012, at 5:28 AM EST, Plymouth Police Department in Indiana were dispatched to Walmart in Plymouth, Indiana in reference to black male subjects that met the description of an investigation on getting money orders from that Walmart with stolen credit cards. Police noticed that the male subjects were in a red Pontiac leaving the parking lot. Plymouth PD pulled the vehicle over, and Kevin Ford and Cortez Stevens was in the car. Kevin Ford stated that he was at Walmart and he was getting a money order. The license plate on the Pontiac was registered to Mercedes Hatcher.

Plymouth Police later learned from Walmart Plymouth that other credit cards had been used at the store for earlier purchases. Video evidence showed Kevin Ford was present at all of these other transactions and Cortez Stevens was present in some of the other transactions. There was also another unknown black male present. These other transactions took place on 1-24-12, 1-25-12, 1-31-12, 2-7-12, 2-10-12, 2-17-12, and 2-18-12 all during the early morning hours. Some of the other purchases included merchandise along with other large purchases of money orders.

Eventually, Plymouth Police Department charged Kevin Ford and Cortez Stevens with theft and credit card fraud on a Citibank account held by TS. Kevin Ford and Cortez Stevens, were arrested for this case by Plymouth PD on 04/20/12. The prosecutor later dropped the initial charge, seeking to charge a higher level felony. The higher level charges were not filed, and Plymouth PD turned their investigation over to the FBI.

TS filed a Regulation E claim with Citibank, indicating the transactions were fraudulent. Citibank denied her claim, because it lacked credibility.

TS told Plymouth PD Detective Leo Mangus that no one had been authorized to use her credit card.

According to the Plymouth Police Department's police report, Ford had a female's credit card in his possession and he stated he had permission to use it.

On the above-listed money orders for KM, the address 700 Greenbay Avenue was listed; on law enforcement database checks, Kevin Ford is also associated with this address (700 Greenbay Ave., Calumet City, IL), for utility listings. KM's name appears on other money orders that were purchased with funds from fraudulent checks that were deposited in this scheme.

## **J. CC Accounts**

On September 9, 2013, at a Citibank branch located in The Lakes, NV, CC opened a checking account (\*\*\*\*\*759) and savings account (\*\*\*\*\*767). Two other Citibank bank accounts (\*\*\*\*\*939 and \*\*\*\*\*947) were opened online on September 19, 2013 in CC's name.

On September 17, 2013, four fraudulent checks were deposited into the four above named accounts owned by CC at a Citibank located at 1525 Ellinwood, Des Plaines, IL. The checks were deposited



between 5:39 PM to 5:41 PM. The deposited checks and what account they were deposited into are detailed below:

Account Deposited In	Check #	Check Date	Amount	Payable to	Payer	Payer's Bank Acct	Date and Time Deposited
*****759	6923	9/19/2013	\$786.45	CC	AMA	Citibank	9/19/2013 5:39 PM
*****767	6922	9/19/2013	\$786.45	CC	AMA	Citibank	9/19/2013 5:40 PM
*****939	6920	9/19/2013	\$786.45	CC	AMA	Citibank	9/19/2013 5:40 PM
*****947	6921	9/19/2013	\$786.45	CC	AMA	Citibank	9/19/2013 5:41 PM
Total			\$3,145.80				

The payer (AMA), as well as the payer's signature, was used on other fraudulent checks that were deposited into other people's accounts. Also, the payer's signature is the same signature that appears on at least \$87,000 worth of fraudulent checks (over 30 checks) that were deposited in the overall scheme starting on December 28, 2011.

Video surveillance shows Kevin Ford depositing the above checks into CC's accounts, using a debit card and PIN. Seconds later, surveillance video shows Ford making ATM withdrawals on CC's accounts, using a debit card and PIN.

Below is a summary of how the proceeds of the fraudulent deposited checks were withdrawn from CC's bank accounts:

**Checking Account- #\*\*\*\*\*947**

Date	Time	Amount Subtracted	Amount Added	Description	Notes
9/19/2013	5:41 PM		\$786.45	Deposit of Fraudulent Check #6921	Occurred at Citibank ATM located at 1525 Ellinwood, Des Plaines, IL
9/19/2013	5:42 PM	\$200.00		Transfer to Checking acct #*****939	Occurred at Citibank ATM located at 1525 Ellinwood, Des Plaines, IL
*9/20/2013	7:59 AM	\$500.00		ATM Withdrawal	Occurred at Citibank ATM located at 2022 S. Archer, Chicago, IL
Totals		\$700.00	\$786.45		

**Checking Account- #\*\*\*\*\*939**

Date	Time	Amount Subtracted	Amount Added	Description	Notes
9/19/2013	5:40 PM		\$786.45	Deposit of Fraudulent Check #6920	Occurred at Citibank ATM located at 1525 Ellinwood, Des Plaines, IL
9/19/2013	5:42 PM		\$200.00	Transfer from Checking acct #*****947	Occurred at Citibank ATM located at 1525 Ellinwood, Des Plaines, IL
9/19/2013	5:42 PM	\$400.00		ATM Withdrawal	Occurred at Citibank ATM located at 1525 Ellinwood, Des Plaines, IL
*9/20/2013	7:58 AM	\$580.00		Transfer to Checking acct #*****759	Occurred at Citibank ATM located at 2022 S. Archer, Chicago, IL
Totals		\$980.00	\$986.45		

**Checking Account- #\*\*\*\*\*759**

Date	Time	Amount Subtracted	Amount Added	Description	Notes
9/19/2013	5:39 PM		\$786.45	Deposit of Fraudulent Check #6923	Occurred at Citibank ATM located at 1525 Ellinwood, Des Plaines, IL
9/19/2013	5:39 PM	\$220.00			Occurred at Citibank ATM located at 1525 Ellinwood, Des Plaines, IL
*9/20/2013	7:58 AM		\$580.00	Transfer from Checking acct #*****939	Occurred at Citibank ATM located at 2022 S. Archer, Chicago, IL
9/20/2013	12:35 PM		\$580.00	Transfer from Savings acct #*****767	Occurred at Citibank ATM located at 8650 S. Stony Island, Chicago, IL
9/20/2013	10:05 AM	\$483.00		ATM Cash Withdrawal	Occurred at Non-Citibank ATM located at 230 W. Grand Ave, Chicago, IL
9/20/2013	12:40 PM	\$1,000.00		Debit PIN Purchase	J Bees Sports & Casual, Chicago, IL
9/20/2013	12:40 PM	\$200.00		Debit PIN Purchase	J Bees Sports & Casual, Chicago, IL



Totals		\$1,903.00	\$1,946.45		
--------	--	------------	------------	--	--

**Savings Account- #\*\*\*\*\*767**

Date	Time	Amount Subtracted	Amount Added	Description	Notes
9/19/2013	5:40 PM		\$786.45	Deposit of Fraudulent Check #6922	Occurred at Citibank ATM located at 1525 Ellinwood, Des Plaines, IL
9/19/2013	5:42 PM	\$200.00			Occurred at Citibank ATM located at 1525 Ellinwood, Des Plaines, IL
9/20/2013	12:35 PM	\$580.00		Transfer from Savings acct #*****759	Occurred at Citibank ATM located at 8650 S. Stony Island, Chicago, IL
Totals		\$780.00	\$786.45		

\*There is video surveillance on September 20, 2013 from 7:57 AM to 7:59 AM at the Citibank ATM located at 2022 S. Archer, Chicago, IL. This surveillance shows Kevin Ford conducting the transactions at the ATM, using a debit card and PIN.

**K. PB Accounts**

On September 18, 2013, at a Citibank branch located in Cypresswood, Texas, PB opened a checking account (\*\*\*\*\*791) and savings account (\*\*\*\*\*801). Two other Citibank bank accounts (\*\*\*\*\*341 and \*\*\*\*\*354) were opened online on September 20, 2013 in PB's name.

On September 20, 2013, four fraudulent checks were deposited into the four above named accounts owned by PB at a Citibank located at 500 W. Madison, Chicago, IL. The checks were deposited between 4:57 PM to 4:59 PM. The deposited checks and what account they were deposited into are detailed below:

Account Deposited In	Check #	Check Date	Amount	Payable to	Payer	Payer's Bank Acct	Date and Time Deposited
*****354	6960	9/17/2013	\$784.45	PB	AMA	Citibank	9/20/2013 4:57 PM
*****801	6900	9/17/2013	\$784.45	PB	AMA	Citibank	9/20/2013 4:58 PM
*****341	6961	9/17/2013	\$784.45	PB	AMA	Citibank	9/20/2013 4:58 PM
*****791	6963	9/17/2013	\$784.45	PB	AMA	Citibank	9/20/2013 4:59 PM
Total			\$3,137.80				

The payer (AMA), as well as the payer's signature, was used on other fraudulent checks that were deposited into other people's accounts.

Below is a summary of how the proceeds of the fraudulent deposited checks were withdrawn from PB's bank accounts:

**Checking Account- #\*\*\*\*\*341**

Date	Time	Amount Subtracted	Amount Added	Description	Notes
9/20/2013	4:58 PM		\$784.45	Deposit of Fraudulent Check #6961	Occurred at Citibank ATM located at 500 W. Madison, Chicago, IL
9/20/2013	4:59 PM	\$200.00		Transfer to Checking acct #*****791	Occurred at Citibank ATM located at 500 W. Madison, Chicago, IL
9/21/2013	8:31 AM	\$580.00		Transfer to Checking acct #*****791	Occurred at Citibank ATM located at 8650 S. Stony Island, Chicago, IL
Totals		\$780.00	\$784.45		

**Checking Account- #9793828654**

Date	Time	Amount Subtracted	Amount Added	Description	Notes
9/20/2013	4:57 PM		\$784.45	Deposit of Fraudulent Check #6960	Occurred at Citibank ATM located at 500 W. Madison, Chicago, IL
9/20/2013	4:59 PM	\$200.00		Transfer to Checking acct #*****791	Occurred at Citibank ATM located at 500 W. Madison, Chicago, IL



9/21/2013	8:32 AM	\$580.00		Transfer to Checking acct #*****791	Occurred at Citibank ATM located at 8650 S. Stony Island, Chicago, IL
Totals		\$780.00	\$784.45		

## Checking Account- #\*\*\*\*\*791

Date	Time	Amount Subtracted	Amount Added	Description	Notes
9/20/2013	4:59 PM		\$784.45	Deposit of Fraudulent Check #6963	Occurred at Citibank ATM located at 500 W. Madison, Chicago, IL
9/20/2013	4:59 PM		\$200.00	Transfer from Checking acct #*****341	Occurred at Citibank ATM located at 500 W. Madison, Chicago, IL
9/20/2013	4:59 PM		\$200.00	Transfer from Checking acct #*****354	Occurred at Citibank ATM located at 500 W. Madison, Chicago, IL
9/20/2013	5:00 PM	\$600.00		ATM Cash Withdrawal	Occurred at Citibank ATM located at 500 W. Madison, Chicago, IL
9/21/2013	8:31 AM		\$580.00	Transfer from Checking acct #*****341	Occurred at Citibank ATM located at 8650 S. Stony Island, Chicago, IL
9/21/2013	8:31 AM	\$500.00		ATM Cash Withdrawal	Occurred at Citibank ATM located at 8650 S. Stony Island, Chicago, IL
9/21/2013	8:32 AM		\$580.00	Transfer from Checking acct #*****354	Occurred at Citibank ATM located at 8650 S. Stony Island, Chicago, IL
9/21/2013	8:32 AM		\$560.00	Transfer from Checking acct #*****801	Occurred at Citibank ATM located at 8650 S. Stony Island, Chicago, IL
9/21/2013	8:32 AM	\$500.00		ATM Cash Withdrawal	Occurred at Citibank ATM located at 8650 S. Stony Island, Chicago, IL
Totals		\$1,600.00	\$2,904.45		

## Savings Account- #\*\*\*\*\*801

Date	Time	Amount Subtracted	Amount Added	Description	Notes
------	------	-------------------	--------------	-------------	-------

9/20/2013	4:58 PM		\$784.45	Deposit of Fraudulent Check #6900	Occurred at Citibank ATM located at 500 W. Madison, Chicago, IL
9/20/2013	5:00 PM	\$220.00		ATM Cash Withdrawal	Occurred at Citibank ATM located at 500 W. Madison, Chicago, IL
9/21/2013	8:32 AM	\$560.00		Transfer to Checking acct #*****791	Occurred at Citibank ATM located at 8650 S. Stony Island, Chicago, IL
Totals		\$780.00	\$784.45		

There is no video surveillance for the deposits, or the withdrawals. However, the same checks were used in the CC's transactions, as well as PB's deposits occurred on the same day as CC's withdrawals. Also, the payer's signature is the same signature that appears on at least \$87,000 worth of fraudulent checks (over 30 checks) that were deposited in the overall scheme starting on December 28, 2011.

#### **FDIC Information**

42. I have obtained certificates issued by the Federal Deposit Insurance Corporation that confirm that the deposits of Citibank, US Bank, JP Morgan Chase Bank, and Bank of America were insured by the Federal Deposit Insurance Corporation during the time period that the transactions outlined herein occurred.


#### **Conclusion**

43. Based upon the information set forth in this affidavit, I believe there is probable cause to believe that, from in or about August 2011 and continuing through in or about September 2013, in the Northern District of Indiana and elsewhere, Kevin Ford, Mercedes Hatcher, Cortez Stevens, Stephen Garner, Brittany Sims, and Mikcale Smally did knowingly conspire to participate in a scheme to defraud or a financial institution and to obtain money and funds owned by and under the custody and control of a financial institution by means of materially false and fraudulent pretenses, representations, and promises, and by concealment of



material facts, in violation of Title 18, United States Code, Sections 371 (conspiracy) and 1344 (bank fraud).

FURTHER AFFIANT SAYETH NOT.

  
Adria Johnson  
Special Agent  
Federal Bureau of Investigation

Sworn and subscribed before me this 23<sup>rd</sup> day of October, 2014.

**S/John E. Martin**  
\_\_\_\_\_  
John E. Martin  
U.S. Magistrate Judge  
Northern District of Indiana